CONTENTS

PARAGRAPH PAGE

FOREWORD

1. The National Imagery Transmission Format Standards (NITFS) is the standard for formatting digital imagery and imagery-related products and exchanging them among members of the Intelligence Community (IC) as defined by Executive Order 12333, the Department of Defense (DOD), and other departments and agencies of the United States Government as governed by Memoranda of Agreement (MOA) with those departments and agencies.

2. The National Imagery Transmission Format Standards Technical Board (NTB) developed this standard based upon currently available technical information.

3. The DOD and members of the Intelligence Community are committed to interoperability of systems used for formatting, transmitting, receiving, and processing imagery and imagery-related information. This standard describes the TActical COmmunication protocol 2 (TACO2) requirements and establishes its application within the NITFS.

4. As a result of a Defense Information Systems Agency (DISA) action, standards for all military data communication protocols will be published in a MIL-STD-2045 series of documents. A MIL-STD-2045 document series has been established within the Data Communications Protocol Standards (DCPS) standardization area.

a. MIL-STD-2045-10000 series. MIL-STD-2045-10000 to MIL-STD-2045-19999 inclusive, will be used to describe DOD's implementation of commercial, international, national, federal, and military standards within the functional profile concept, in order to provide required network services. U.S. Government Open Systems Interconnection Profile (GOSIP) will be the basis for developing the 10000 series with DOD enhancements and unique military standards.

b. MIL-STD-2045-20000 series. MIL-STD-2045-20000 to MIL-STD-2045-29999 inclusive, will be used to describe DOD enhancements and extensions to existing commercial, international, national, or federal standards.

c. MIL-STD-2045-30000 series. MIL-STD-2045-30000 to MIL-STD-2045-39999 inclusive, will be used to describe DOD unique protocols and services that are not supported by commercial, international, national, or federal standards.

CONTENTS

PARAGRAPH PAGE

d. MIL-STD-2045-40000 series. MIL-STD-2045-40000 to MIL-STD-2045-49999 inclusive, will be used to document interim standards. Interim standards are documents DOD needs until these standards are described in either GOSIP or MIL-STD-2045-20000 or 30000 series standards.

5. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Organization (JIEO), Center for Standards (CFS), Attn: TBBD, Fort Monmouth, NJ 07703-5613 by using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

TABLE OF CONTENTS.

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

PARAGRAPH PAGE

FIGURE

CONTENTS

1. SCOPE

1.1 Scope. This document establishes the requirements for the TActical COmmunications protocol 2 (TACO2), part of the National Imagery Transmission Format Standards (NITFS). National Imagery Transmission Format (NITF) is a standard format for transmitting digital imagery and imagery-related products among members of the Intelligence Community, and TACO2 is a protocol suite that may be used for that transmission. It includes requirements for Forward Error Correction (FEC), which is necessary to ensure interoperability and to promote commonality among subsystems that comply with NITFS.

1.2 Content. This standard establishes the requirements to be met by systems complying with NITFS when using the TACO2 protocol, and defines the protocols and formats that make up TACO2. All aspects of TACO2 that affect functional interoperability are specified herein. In addition, guidance is provided for those aspects of TACO2 operation that are not strictly related to interoperability but may

affect technical performance or resistance to error.

1.3 Applicability. This standard is applicable to the Intelligence Community and the DOD. It is mandatory for all Secondary Imagery Dissemination Systems (SIDS) in accordance with the memorandum by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence ASD(C^3I), Subject: National Imagery Transmission Format Standards (NITFS), 12 August 1991. This directive shall be implemented in accordance with JIEO Circular 9008, and MIL-HDBK-1300. New equipment and systems, those undergoing major modification, or those capable of rehabilitation shall conform to this standard.

1.4 Protocol tailoring. TACO2 is designed as a single protocol stack that provides for message transfer over a wide variety of tactical communication circuits. It is particularly appropriate for use over circuits where other protocol suites operate poorly or not at all, but also is designed to perform well over any communications circuit. It can transfer any form of data, since it does not use any internal component of an NITFS message. It can be configured to operate over circuits not anticipated at initial installation; therefore, a conforming TACO2 implementation must implement all capabilities specified herein, except as specifically noted. The possible ranges of various parameters may be limited for specific applications; mandatory ranges are specified in this document. Additional information on NITFS compliance is available in JIEO Circular 9008.

1.5 FEC tailoring. As a minimum, only those features or functions specified herein, necessary to ensure interoperability among systems, shall be implemented in an equipment item. While every effort has been made to include all the features necessary, certain aspects depend on system application and must be tailored by the specification writer. These aspects include:

a. User choice of appropriate FEC selection.

b. Automatic switching of FEC code based on the conditions of the tactical line.

c. Inhibiting external or internal FEC codes.
d. Using an external FEC code if it is desired.

2. APPLICABLE DOCUMENTS

2.1 Government documents.

2.1.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the issue of the Department of Defense Index of Specifications and Standards (DODISS) and supplements thereto, cited in the solicitation.

STANDARDS

FEDERAL

FED-STD-1037B	-	Telecommunications: Glossary of Telecommunication Terms, 3 June 1991.

MILITARY

MIL-STD-1777	-	Military Standard Internet Protocol, Defense Communications Agency, August 1983.
MIL-STD-188-114A	-	Electrical Characteristics of Digital Interface Circuits, 30 September 1985.
MIL-STD-2500	-	National Imagery Transmission Format (NITF) for the National Imagery Transmission Format Standards (NITFS), 18 June 1993.

HANDBOOKS

MIL-HDBK-1300	-	National Imagery Transmission Format Standards (NITFS), 18 June 1993.

(Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from the Standardization Documents Order Desk, 700 Robbins Avenue, Building #4, Section D, Philadelphia, PA 19111-5094.)

2.1.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified. Unless otherwise specified, the issues are those cited in the solicitation.

DISA/JIEO Circular 9008	-	NITFS Certification Test and Evaluation Plan, (Effectivity 8).
DISA/JIEO SPEC 9137	-	NITFS TACO2 Protocol to KY-57/58 Cryptographic Device Technical Interface Specification (TIS), (Effecitivity 8).
DISA/JIEO SPEC 9138	-	NITFS TACO2 Protocol to KG-84-A/C Cryptographic Device Technical Interface Specification (TIS), (Effectivity 8).

DISA/JIEO SPEC 9139	-	NITFS TACO2 Protocol to KY-68 Cryptographic Device Technical Interface Specification (TIS), (Effectivity 8).
DISA/JIEO SPEC 9140	-	NITFS TACO2 Protocol to STU-III Cryptographic Device Technical Interface Specification (TIS), (Effectivity 8).

(Copies of DISA/JIEO Specifications may be obtained from DISA/JIEO/CFS/TBB, Fort Monmouth, NJ 07703-5613. Copies of DISA/JIEO Circular 9008 may be obtained from DISA/JIEO/JITC, Fort Huachuca, AZ 85613-7020.)

2.2 Non-Government publications. The following document(s) form a part of this document to the extent specified herein. Unless otherwise specified, the issues of the documents which are DOD adopted are those listed in the issue of the DODISS cited in the solicitation. Unless otherwise specified, the issues of documents not listed in the DODISS are the issues of the documents cited in the solicitation.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

ISO 3309	-	High-Level Data Link Control Procedures - Frame Structure, International Organization for Standardization, Switzerland, 15 January 1992.
ISO 7498	-	Open systems interconnection - basic reference model International Organization for Standardization, Switzerland.
ISO 8825	-	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), International Organization for Standardization, Switzerland, 15 December 1990.
ISO 9171	-	Recorded/Unrecorded Characteristics of 130 mm Optical Disk Cartridges.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI X3.4-1986	-	American National Standard Code for Information Interchange (ASCII), 1986.

INTERNET RFCs

RFC 791	-	Internet Protocol, Postel, J.B., 1981.
RFC 792	-	Internet Control Message Protocol, Postel, J.B., 1981.
RFC 919	-	Broadcasting Internet datagrams, Mogul, J.C., 1984.
RFC 922	-	Broadcasting Internet datagrams in the presence of subnets, Mogul, J.C., 1984.
RFC 950	-	Internet standard subnetting procedure, Mogul, J.C.; Postel, J.B., 1985.
RFC 998	-	NETBLT: A bulk data transfer protocol, Clark, D.D.; Lambert, M.L.; Zhang, L., 1987.
RFC 1055	-	Nonstandard for transmission of IP datagrams over serial lines: SLIP, Romkey, J.L., 1988.
RFC 1108	-	Security Options for the Internet Protocol, Kent, S., 1991.
RFC 1112	-	Host extensions for IP multicasting, Deering, S.E., 1989.

(Non-Government standards and publications are usually available from the organization that prepare or distribute the documents. These documents also may be available in or through libraries or other informational services.)

2.3 Order of precedence. In the event of a conflict between the text of this standard and the references cited herein, the text of this standard takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 Acronyms used in this standard. The following definitions are applicable for the purpose of this standard. In addition, terms used in this standard and defined in the FED-STD-1037B shall use the FED-STD-1037B definition unless noted.

a.	ANSI	American National Standards Institute
b.	ASCII	American Standard Code for Information Interchange
c.	ASD(C^3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
d.	ASN.1	Abstract Syntax Notation One
e.	BCH	Bose-Chaudhuri-Hocquenghem
f.	BER	Bit Error Ratio
g.	BERT	Bit Error Ratio Test
h.	BPSK	Binary Phase Shift Keying
i.	CCITT	International Telegraph and Telephone Consultative Committee
j.	CFS	Center for Standards
k.	CRC	Cyclic Redundancy Check
l.	DAMA	Demand Assignment Multiple Access
m.	DCE	Data Circuit-terminating Equipment
n.	DCPS	Data Communications Protocol Standards
o.	DDN	Defense Data Network
p.	DISA	Defense Information Systems Agency (formerly DCA)
q.	DISN	Defense Information Systems Network (formerly DDN)
r.	DOD	Department of Defense

s.	DODISS	Department of Defense Index Specifications and Standards
t.	DTE	Data Terminal Equipment
u.	EDAC	Error Detection and Correction
v.	EDAC	Error Detection and Correction
w.	FCS	Frame Check Sequence
x.	FEC	Forward Error Correction
y.	FTP	File Transfer Protocol
z.	GOSIP	U.S. Government OSI Profile
aa.	HDLC	High-level Data Link Control
ab.	HF	High Frequency
ac.	IC	Intelligence Community
ad.	ICMP	Internet Control Message Protocol
ae.	IHL	Internet Header Length
af.	IP	Internet Protocol
ag.	ISO	International Organization for Standardization
ah.	JIEO	Joint Interoperability and Engineering Organization (formerly JTC3A)
ai.	LSB	Least Significant Bit
aj.	LOS	Line of Sight
ak.	MBZ	Must Be Zero
al.	MOA	Memoranda of Agreement

am.	MSB	Most Significant Bit
an.	msec	Milliseconds
ao.	NETBLT	NETwork BLock Transfer
ap.	NITF	National Imagery Transmission Format
aq.	NITFS	National Imagery Transmission Format Standards
ar.	NRTS	National Imagery Transmission Format Reliable Transfer Server
as.	NTB	National Imagery Transmission Format Standard Technical Board
at.	OSI	Open Systems Interconnection
au.	RFC	Request for Comment (Internet environment)
av.	SID	Secondary Imagery Dissemination
aw.	SIDS	Secondary Imagery Dissemination System
ax.	SLIP	Serial Line Internet Protocol
ay.	TACO2	TActical COmmunications protocol 2
az.	TBR	To Be Resolved
ba.	TCP	Transmission Control Protocol
bb.	TIS	Technical Interface Specification
bc.	TRI-TAC	Tri-Service Tactical Communications
bd.	UDP	User Datagram Protocol
be.	UHF	Ultra High Frequency
bf.	UID	Unique Identifier
bg.	VHF	Very High Frequency

bh. UI Unnumbered Information

3.2 Definitions used in this standard. The definitions used in this document are defined as follows:

a. Bit error ratio test (BERT) - A function or sequence of functions that compares a received data pattern with a known transmitted pattern to determine the level of transmission quality. Note: Can be used as an adjective, for example, "Bit error ratio test packets" are packets used in a bit error ratio test.

b. Bit-stuffing - For NITFS, in High-level Data Link Control (HDLC), a technique used to avoid spurious appearances of the flag within a frame.

c. Bose-Chaudhuri-Hocquenchem (BCH) codes - An important class of binary, block forward error correction (FEC) codes. BCH codes offer a great deal of flexibility in terms of code rate and block length. Hamming codes may be thought of as single error-correcting BCH codes.

d. Byte - A sequence of N adjacent binary digits, usually treated as a unit, where N is a non zero integral number. Note: In pre-1970 literature, "byte" referred to a variable length field. Since that time the usage has changed so that now it almost always refers to an 8-bit field. This usage predominates in computer and data transmission literature; throughout this document, the term is synonymous with "octet."

e. Byte-stuffing - A procedure in which either the Huffman coder or the arithmetic coder inserts a zero byte into the entropy-coded segment following the generation of an encoded hexadecimal 0xFF byte. For the purpose of NITFS, in Serial Line Internet Protocol (SLIP), a technique used to avoid spurious appearances of the END character within a frame.

f. Client - An executing program or protocol layer that requests or receives services from a lower protocol layer.

g. Criticality - Those portions of a message which must be received correctly for the message to be useful are considered critical. Criticality provides a means for identifying those portions of a message.

h. Datagram - In packet-switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment to the destination data terminal equipment, without relying on earlier exchanges between the equipment and the network. Note: Unlike virtual call service, there are no call establishment or clearing procedures, and the network does not generally provide protection against loss, duplication, or misdelivery.

i. Data link layer - Layer two in the ISO OSI Reference Model. The role of the data link layer is to group the bits of the physical layer into frames, and to deal with transmission errors to allow the sending of frames between adjacent nodes in the network.

j. Duplex - For the purpose of this MIL-STD, an operational mode in which frames may be transferred across a link in both directions; i. e., half-duplex or full-duplex.

k. Effectivity - Some of the capabilities specified in this document are not required as of the issue date of the document. All such capabilities are marked with effectivity numbers, for example, (Effectivity 1). Each effectivity number will be replaced by a specific date in subsequent releases of this document.

l. Embedded FEC - For the purpose of this MIL-STD, FEC is an element of a hardware unit with more general functionality.

m. Error Detection and Correction (EDAC) - The application of one or several methods for the detection and correction of errors in a bit stream. For the purpose of this MIL-STD, EDAC generally is used synonymously with FEC, but is sometimes used to refer to error control systems that make use of a backward channel (for example, retransmission requests).

n. Finite field - See Galois field.

o. Forward Error Correction (FEC) - A system of error control for data code transmission wherein the receiving device has the capability to detect and correct any character or block that contains fewer than a predetermined number of symbols in error. Note: FEC is accomplished by adding bits to each transmitted character or code block using a predetermined algorithm.

p. Frame - 1. For the purpose of this MIL-STD, in data transmission, a sequence of contiguous bits bracketed by and including uniquely recognizable delimiters. 2. For the MIL-STD-188-198 (JPEG), a group of one or more scans (all using the same DCT-based or lossless process) through the data of one or more of an image.

q. Full duplex - For the purpose of this MIL-STD, an operational mode in which frames may be simultaneously transferred across a link in both directions. A TACO2 connection supports image transmission in only one direction at a time; return frames contain control information only.

r. Galois field - An algebraic structure commonly used for error correction and cryptographics calculations. A Galois field is a field whose set of elements is finite. The field operations of addition, subtraction, multiplication, and division are defined.

s. International Organization for Standardization (ISO) - A global standards body.

t. ISO OSI Reference Model - A seven layer protocol stack defined by the ISO.

u. Keepalive - A signal whose purpose is to inform a process that a connection is still in operation.

v. Metamessage - A collection of information related to a NITF message, which is transmitted in association with the message.

w. Modem - Acronym for Modulator-Demodulator. A device that modulates and demodulates signals. Note: 1. Modems are primarily used for converting digital signals into quasi-analog signals for transmission over analog communication channels and for reconverting the quasi-analog signals into digital signals. Note: 2. Many additional functions may be added to a modem to provide for customer service and control features.

x. Multicast - Transmission of a single message to a group of receivers.

y. Network layer - Layer three in the ISO OSI Reference Model. The role of the network layer is to transfer packets from their source node to their destination node by hopping through the intermediate nodes.

z. Octet - A byte of eight binary digits usually operated upon as an entity.

aa. Packet - In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and possibly error control information are arranged in a specific format.

ab. Physical layer - Layer one in the ISO OSI Reference Model. The role of the physical layer is that of raw transmission of unformatted information.

ac. Port - For the NITFS, the identifier that transport protocols use to distinguish among multiple destinations in a host computer.

ad. Protocol stack - A set of multiple layers that describe the function of a network or communication system with the uppermost layer is being associated with the application and the lowest layer's being associated with the physical communications channel.

ae. Reed-Solomon code - For the purpose of NITF, a class of FEC codes in which the input and output symbols are multi-bit symbols and are treated as Finite Field elements.

af. Simplex - For NITFS, providing transmission in only one preassigned direction.

ag. Validity - Validity provides a means of identifying those portions of a message known to contain possible errors.